



# FICAM Initiative Highlights: Spring 2013

*“Our ability to properly protect information as it is shared is directly related to the maturity of governance processes, access controls, identity management, enterprise audit capabilities, and network interoperability efforts.”*

– The National Strategy for Information Sharing and Safeguarding, December 2012

## Spring 2013 ICAM Day at a Glance

Today's event includes presentations, panel discussions, and breakout sessions for collaborative discussions on the pressing issues facing the Federal Government's ICAM programs today.

### Current Trends

### ICAM Day Take Aways

#### Driving Efficiencies & Cost Savings



- Heightened focus on consolidating IT investments through investments in enterprise ICAM solutions
- Efforts are underway to promote use of existing services & identify new shared services

- ✓ Evaluate opportunities to reduce costs through enterprise ICAM capabilities
- ✓ Leverage existing investments

#### Continued Implementation of HSPD-12



- Significant investment has been made by agencies to issue PIV cards
- The focus is shifting from issuance to fully leveraging the PIV card's security features to provide strong identity assurance in an interoperable manner

- ✓ Plan for & enable IT systems to use the PIV card for access
- ✓ Leverage guidance & best practices from the FICAM Roadmap

#### Information Sharing & Attribute Exchange



- Work is underway for the use of access control attributes across the Federal Government
- Partners are actively being sought after for the initial use of the BAE capability

- ✓ Explore dynamic access control models (e.g., ABAC)
- ✓ Contribute to the development of the FICAM Attribute Roadmap

#### Mobile Security & Authentication



- Mobile device management is a priority with the growing demand for “bring-your-own-device” within agencies
- Baseline security controls & profiles and requirements are under development

- ✓ Define mobile device policy & architecture to meet security requirements
- ✓ Stay tuned for new PIV-derived credential guidance

#### ICAM Solution Design & Procurement



- Coordination is underway with the ICAM vendor community to improve the inclusion of ICAM requirements into product offerings
- More integrated and interoperable solutions have been added to the FICAM Testing Program

- ✓ Use the FICAM Testing Program to help specify procurement requirements
- ✓ Socialize procurement changes with procurement officers

#### PIV-enabled Physical Security



- Attention is focused on use of strong authentication mechanisms that meet the vision of the ICAM segment architecture
- Work is underway to reconcile and updated guidance to physical security professionals to upgrade physical access control systems

- ✓ Plan for & enable the use of the PIV card for physical access to federal facilities
- ✓ Use the appropriate authentication mechanisms

For more information, please contact [ICAM@gsa.gov](mailto:ICAM@gsa.gov)

# What's Going On?

The ICAMSC has been tackling a variety of work items to support agency efforts in improving their ICAM programs and achieving the target state for ICAM. These work items seek to address identified agency issues and challenges; close policy, procedure, and standards gaps; and provide guidance and services to promote the success of agency ICAM programs.

The new IDmanagement.gov	Leadership Communications Materials	Implementation Plan for FICAM on All Security Domains
A new look and feel, more content, and user-friendly navigation structure offer agencies a single information hub for all things FICAM. <b>Visit the site at <a href="http://idmanagement.gov">idmanagement.gov</a></b>	Extensive slide presentation outlining the intent and value of investment in ICAM to support internal agency meetings to garner leadership buy-in. <b>Available at <a href="http://idmanagement.gov">idmanagement.gov</a></b>	Addresses National Strategy for Information Sharing & Safeguarding Priority Objective #4 to implement FICAM on all security fabrics. <b>Currently under development</b>
Expand ICAM architecture and promote government-wide implementation		

FICAM Testing Program	Mobile Device Authentication Guidance	PIV for Enterprise PACS Guidance
Revamp of the FIPS 201 Evaluation Program to support improved testing of ICAM solutions and procurement of approved ICAM products & services. <b>Visit the site at <a href="http://placeholder.gov">placeholder.gov</a></b>	Defines a current and target state for authenticating users and their mobile devices and a transition roadmap for meeting the target state. <b>Under development by the LAWG</b>	Defines the security controls for a target state Physical Access Control System and authentication patterns using PIV and PIV-I credentials. <b>Pending formal release</b>
Support purchase and implementation of solutions for logical and physical access		

Relying Party Guidance for Accepting Externally-Issued Credentials	FICAM Attribute Management Roadmap	Backend Attribute Exchange (BAE) Capability
Supplemental guidance to the FICAM Roadmap on federation planning, architecture, & implementation. <b>Available on <a href="http://idmanagement.gov">idmanagement.gov</a></b>	Establishes a standardized approach to govern attribute management and exchange and support access control policy decisions. <b>Available on <a href="http://Max.gov">Max.gov</a> to members</b>	Operational capability with common attribute and metadata services compliant with the BAE specification to support flexible information sharing. <b>Contact <a href="mailto:icam@gsa.gov">icam@gsa.gov</a> to sign up</b>
Enable identity federation and attribute exchange across participants		

To view or download the presentations and materials from the April 2013 ICAM Information Sharing Day, please visit:

**[www.idmanagement.gov/news/icam-day-june-2013](http://www.idmanagement.gov/news/icam-day-june-2013)**